ALEX G. TSE (CABN 152348)
Acting United States Attorney

BARBARA J. VALLIERE (DCBN 439353)
Chief, Criminal Division

JOHN H. HEMANN (CABN 165823)
JEFFREY SHIH (MABN 663195)
Assistant United States Attorneys

SCOTT K. MCCULLOCH (DCBN 1020608)
Trial Attorney, National Security Division

450 Golden Gate Avenue, Box 36055
San Francisco, California 94102-3495
john.hemann@usdoj.gov; 415.436.7478
jeffrey.shih@usdoj.gov; 415.436.7168

Attorneys for the United States of America

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA, Plaintiff, v. KARIM BARATOV, Defendant.	CASE NO. 3:17-CR-103 VC UNITED STATES SUPPLEMENTAL SENTENCING MEMORANDUM Sentencing Date: May 29, 2018 Time: 10:30 a.m. Court: Honorable Vince Chhabria

At the sentencing hearing on April 24, 2018, the Court requested further briefing on the sentences of similarly situated federal defendants and the need to avoid unwarranted sentence disparities under 18 U.S.C. § 3553(a)(6). The United States hereby submits further information from sentences coded in United States Sentencing Commission data (Section I) and from sentences identified through other sources (Section II). An analysis of that additional information (Section III) shows that the sentence recommended by the United States for Defendant Baratov is consistent with the sentences imposed on "defendants with similar records who have been found guilty of similar conduct." 18 U.S.C. § 3553(a)(6). Therefore, based on the United States Sentencing Memorandum (Docket No. 36), the

United States Sealed Response (Docket No. 38), the United States Response Memorandum (Docket No. 39), and this supplemental memorandum, the United States respectfully recommends that the Court impose a sentence of 94 months imprisonment, 3 years supervised release, and restitution and fine amounts that encompass any and all of his assets.

I. SENTENCES FROM UNITED STATES SENTENCING COMMISSION DATA

As described in the accompanying Declaration of Assistant United States Attorney Jeffrey Shih ("Shih Decl."), United States Sentencing Commission ("USSC") sentencing data is publicly available and accessible through Microsoft Excel for the fiscal years in 2007 through 2011, and 2014 and 2015. Shih Decl. ¶¶ 3-4.[1] The United States used that data to identify the 19 hacking sentences summarized in the table below. To do so, the United States filtered the USSC sentencing data by using the criminal offense characteristics that Defendant Baratov agrees apply to him, specifically:

a. application of § 2B1.1,

b. the 2-level specific offense characteristic for sophisticated means, and

c. the 2-level specific offense characteristic for committing an offense under 18 U.S.C. § 1030 to obtain personal information.

Shih Decl. ¶¶ 1, 2, 5.

Filtering on the agreed-upon criminal offense characteristics resulted in the following sentences.

Year of Sentence	Loss Increase, 2B1.1(b)(2)	Final Offense Level	Final Criminal History Category	USSG Range Min.	USSG Range Max.	Statutory Min.	Statutory Max.	Prison Sentence	Sentence Relative to USSG Range
2008	+8	23	1	46	57	24	84	72	Within
2009	+4	19	4	46	57	0	720	48	Within
2009	+8	15	1	18	24	0	60	0[2]	Gov't-sponsored
2009	+6	15	1	18	24	24	444	42	Within

[1] As discussed in Paragraphs 3 and 4 of the Shih Declaration, datafiles that could be readily accessed through Microsoft Excel (*i.e.*, tab-delimited format) were available on the website of the University of Michigan's Inter-University Consortium for Political and Social Research ("ICPSR"), which the Sentencing Commission website references. The ICPSR website did not appear to have datafiles available in tab-delimited format for 2012, 2013, 2016, or 2017.

The ICPSR Terms of Use restrict against the use of the data to identify or investigate specific research subjects.

[2] The sentence in this case included 12 months of alternative incarceration. Shih Decl. ¶ 8 n.11.

Year of Sentence	Loss Increase, 2B1.1(b)(2)	Final Offense Level	Final Criminal History Category	USSG Range Min.	USSG Range Max.	Statutory Min.	Statutory Max.	Prison Sentence	Sentence Relative to USSG Range
2010	+22	43	6	Life	Life	48	3708	3708	Within
2010	+18	26	1	63	78	0	600	51	Below
2010	0	22	1	41	51	24	144	132	Above
2011	+6	14	3	21	27	24	324	45	Within
2011	0	12	1	10	16	0	60	0.03[3]	Above
2011	+8	21	1	37	46	0	120	72	Above
2013	+16	31	4	151	188	0	120	120	Within
2013	0	13	1	12	18	24	84	60	Above
2013	+22	43	1	Life	Life	0	300	72	Gov't-sponsored
2013	+22	43	1	Life	Life	0	300	12.03[4]	Gov't-sponsored
2014	+8	17	1	24	30	0	120	0	Gov't-sponsored
2014	+4	12	4	21	27	0	60	15	Gov't-sponsored
2014	+12	19	1	30	37	0	60	0[5]	Below
2014	+4	13	1	12	18	0	60	18	Within
2014	0	18	1	27	33	0	120	9	Gov't-sponsored
2014	+20	31	4	151	188	0	120	48	Gov't-sponsored
2015	+16	26	4	92	115	0	300	72	Below
2015	+24	40	1	292	365	0	780	156	Gov't-sponsored
2015	+12	31	1	108	135	0	120	54	Gov't-sponsored

Shih Decl. ¶¶ 6-12. The sentences in light grey were "Gov't-sponsored" sentences below the Guidelines range for 5K1.1/substantial assistance, 5K3.1/early disposition, and other government-sponsored reasons.

[3] The sentence in this case included 18 months of alternative incarceration. Shih Decl. ¶ 10 n.13.
[4] The sentence in this case included 6 months of alternative incarceration. Shih Decl. ¶ 11 n.14.
[5] The sentence in this case included 6 months of alternative incarceration. Shih Decl. ¶ 11 n.15.

II. DESCRIPTIONS OF SENTENCES FROM OTHER SOURCES

The United States also identified sentences in hacking cases through other sources, such as press releases and information available on PACER. Generally, the cases fell into two categories: "carding" cases, and non-carding cases.

"Carding" hacking cases typically involved the wholesale theft of customer credit card data from businesses—often nationwide retailers—and the subsequent misuse and resale of this data. Because cybercriminals conducting such thefts often download every credit card number in a victim business's database, carding cases typically involve tens or hundreds of thousands of victims, who face financial losses from having their credit cards stolen and misused. For a carding case, even for a single hacking, the loss amount may thus depend primarily on the amount of data on the victim server. Individual carding victims are typically not liable for fraudulent charges if those charges are identified, but losses are borne by banks or insurers.

In non-carding cases, cybercriminals typically target fewer victims (when compared to the tens or hundreds of thousands of victims in carding cases), but exploit the breaches of personal data beyond credit card misuse. Victims in such cases face, for example, massive financial harm from loss of business information or financial account contents, personal harms of a significant and lasting nature, and other significant intrusion effects.

Examples of each type of case follow below.

A. Carding Cases

1. *United States v. Salcedo*, 5:03-cr-53-LHT (W.D.N.C. Dec. 15, 2004)[6]

Brian Salcedo and a coconspirator parked outside a Lowe's home improvement store in Southfield, Michigan and tapped into the store's unsecured WiFi network. Over the course of weeks, they used that foothold to penetrate Lowe's servers at stores across the country, where they eventually planted software that stole customer credit card numbers as such numbers were transmitted from cash registers to a processing server in North Carolina. The court granted the government's motion for a downward departure based on the fact that after pleading guilty, the defendant helped Lowe's understand the vulnerabilities in its system. *See* Judgment (Dkt. 29); Government's Motion for

[6] These dates indicate the date of the sentencing.

Downward Departure Pursuant to U.S.S.G. § 5k1.1 (Dkt. 26); https://www.justice.gov/archive/criminal/cybercrime/press-releases/2004/salcedoSent.htm.

- Offenses: One count of conspiracy to commit computer fraud, three counts of computer fraud
- Guidelines Range: 121-151 months
- Sentence: 108 months

2. *United States v. Butler*, 07-cr-332-MBC (W.D. Pa. Feb. 12, 2010)

Max Ray Butler hacked into financial institutions, credit card processing centers, and other secure computers in order to acquire credit card account information and other personal identification information. Many of these credit card numbers were provided to an accomplice who, along with a team of associates, used fake cards encoded with the stolen numbers to buy merchandise for resale. Butler sold the rest of the card numbers outright over the Internet. Butler and his accomplice also created a website known as "CardersMarket," devoted to the acquisition, use, and sale of credit card account information. A primary purpose of the site was to recruit talented individuals to assist in carding activity. At its peak, CardersMarket had approximately 4,500 members worldwide. *See* Judgment (Dkt. 70); Sentencing Minute Entry (Dkt. 69); Government's Sentencing Memorandum (Dkt. 66); https://archives.fbi.gov/archives/pittsburgh/press-releases/2010/pt021210b.htm.

- Offenses: Two counts of wire fraud
- Guidelines Range: 360 months to life (prior to 5k1.1 motion)
- Sentence: 156 months

3. *United States v. Gonzalez*, 1:08-cr-10223-PBS (D. Mass. Mar. 25, 2010)

This sentence is for two criminal cases, which were consolidated, that concern hacks into retailer TJX, Office Max, Dave & Buster's restaurant chain, Barnes & Noble, and a string of other companies. Albert Gonzalez and his coconspirators hacked into a local TJX outlet's network and used this foothold to obtain unauthorized access to its corporate network in Massachusetts. They then installed malware on the TJX network to siphon transaction data in real time, including the magnetic stripe data from credit and debit cards. The stolen magnetic stripe data was routed to servers Gonzalez leased in Latvia and Ukraine, and was ultimately passed to a notorious Ukrainian card seller, who peddled them to other cybercriminals. Gonzalez's offenses yielded millions of victims and approximately $200 million in

losses to myriad businesses. *See* Sentencing Transcript (Dkt. 94); Government's Sentencing Memorandum (Dkt. 85); Third Amended Judgment (Dkt. 103); https://www.justice.gov/opa/pr/leader-hacking-ring-sentenced-massive-identity-thefts-payment-processor-and-us-retail.

- Offenses: One count of conspiracy to commit computer fraud, and multiple substantive counts of aggravated identity theft and computer, wire, and access device fraud.
- Guidelines Range: life
- Sentence: 240 months

4. *United States v. Bendelladj*, 1:11-cr-00557-AT-AJB (N.D. Ga. Apr. 20, 2016)

Hamza Bendelladj and his coconspirators developed and marketed SpyEye, which was the preeminent malware banking Trojan from 2010-2012. SpyEye was designed to automate the theft of confidential personal and financial information, such as online banking credentials, credit card information, usernames, passwords, PINs, and other personally identifying information. Using SpyEye, Bendelladj stole personal identifying information from close to half a million people and hundreds of thousands of credit card and bank account numbers, causing millions of dollars in losses to individuals and financial institutions. Bendelladj also ran a website where he automated the sale of stolen credit card information. *See* Sentencing Transcript (Dkt. 214); Judgment (Dkt. 192); https://www.justice.gov/usao-ndga/pr/two-major-international-hackers-who-developed-spyeye-malware-get-over-24-years-combined.

- Offenses: 23 counts of computer, wire, and bank fraud
- Guidelines Range: 188-235 months
- Sentence: 180 months

5. *United States v. Seleznev*, 2:11-cr-00070-RAJ (W.D. Wa. April 21, 2017)

Between October 2009 and October 2013, Roman Seleznev hacked into retail point-of-sale systems and installed malware that allowed him to steal millions of credit card numbers from more than 500 U.S. businesses and send the data to servers that he controlled in Russia, the Ukraine, and McLean, Virginia. Seleznev then bundled the credit card information into groups called "bases" and sold the information on various criminal carding websites to buyers who used them for fraudulent purchases. Evidence presented at trial showed that Seleznev's scheme caused approximately 3,700 financial

institutions more than $169 million in losses, and that Seleznev earned tens of millions of dollars from his criminal activity. *See* Sentencing Transcript (Dkt. 478); Amended Judgment (Dkt. 479); https://www.justice.gov/opa/pr/russian-cyber-criminal-sentenced-27-years-prison-hacking-and-credit-card-fraud-scheme.

- Offenses: Ten counts of wire fraud, 17 counts of computer fraud, nine counts of access device fraud, and two counts of aggravated identity theft
- Guidelines Range: life
- Sentence: 324 months

6. *United States v. Tverdokhlebov*, 1:17-cr-9-TSE (E.D. Va. July 10, 2017)

Alexander Tverdokhlebov operated several "botnets," which are groups of compromised computers that can be used for a variety of malicious purposes, including to steal credit card and other sensitive financial information. At various points, he claimed to have possessed 40,000 stolen credit card numbers and to have been able to control up to 500,000 infected computers. Tverdokhlebov sold this stolen financial information to other cybercriminals and enabled his associates to make fraudulent purchases or withdrawals from victims' accounts. He also laundered money for other Russian-speaking cybercriminals. *See* Judgment (Dkt. 61); Sentencing Minute Entry (Dkt. 58); Government's Amended Sentencing Memorandum (Dkt. 54); https://www.justice.gov/usao-edva/pr/russian-born-cybercriminal-sentenced-over-nine-years-prison.

- Offense: One count of wire fraud
- Guidelines Range: 97-121 months
- Sentence: 110 months

B. Non-Carding Cases

1. *United States v. Makwana*, 1:09-cr-00043-JFM (D. Md. Dec. 17, 2010)

Rajendrasinh Makwana was a UNIX engineer contractor for Fannie Mae, who worked on Fannie Mae's network of almost 5,000 computer servers. Makwana was fired on October 24, 2008 and told to turn in all of his Fannie Mae equipment, including his laptop. That day, Makwana transmitted malicious code designed to propagate throughout the Fannie Mae network of computers and destroy all data, including financial, securities and mortgage information. However, Makwana accidentally altered the

code, thereby frustrating his own plan. *See* Judgment (Dkt. 62); Press release, https://www.justice.gov/archive/usao/md/news/archive/FannieMaeCorporateIntruderSentencedtoover3YearsforAttemptingtoWipeoutFannieMaeFinancialData.html.

- Offense: One count of computer fraud
- Guidelines Range: 41-51 months
- Sentence: 41 months

2. *United States v. Chaney*, 2:11-cr-00958-SJO (C.D. Cal. Dec. 17, 2012)

Christopher Chaney hacked into the personal email accounts of approximately 60 people—mostly celebrities—and stole intimate photographs and other documents. While he had control of the email accounts, he changed the account settings so that copies of all emails would be surreptitiously forwarded to an alias email account he controlled. Ultimately, Chaney forwarded many of the stolen photographs to third-party websites, which resulted in some being posted to the Internet, including the sexually explicit photographs of a young Disney actress who then attempted suicide. Chaney demonstrated significant recidivism risk and was facing potential child pornography charges in another district. *See* Plea Agreement (Dkt. 32); United States' Sentencing Memorandum (Dkt. 36); United States' Response to Defendant's Sentencing Memorandum (Dkt. 59); Judgment (Dkt. 84); Sentencing Transcript (Dkt. 96); Press release, https://archives.fbi.gov/archives/losangeles/press-releases/2012/florida-man-convicted-in-wiretapping-scheme-targeting-celebrities-sentenced-to-10-years-in-federal-prison-for-stealing-personal-data.

- Offenses: Six counts of computer fraud and three counts of wiretapping
- Guidelines Range: 57-71 months
- Sentence: 120 months

3. *United States v. Musacchio*, 3:10-cr-00308-P-1 (N.D. Tx. Sept. 5, 2013)

Michael Musacchio was the president of Exel Transportation Services, a third-party logistics or intermodal transportation company. In 2004, Musacchio left Exel to form a competing company, Total Transportation Services, where he was the original president and CEO. Two other former Exel employees from the Exel IT Department also went to work at Musacchio's new company. Between 2004 and 2006, Musacchio and the IT employees engaged in a scheme to hack into Exel's computer

system for the purpose of conducting corporate espionage. Through their repeated unauthorized accesses into Exel's email accounts, Musacchio and one employee were able to obtain Exel's confidential and proprietary business information and use it to benefit their new employer and themselves as investors. *See* Sentencing Transcript pt. 1 (Dkt. 238); Sentencing Transcript pt. 2 (Dkt. 255); Press release, https://www.justice.gov/usao-ndtx/pr/plano-texas-man-sentenced-63-months-federal-prison-corporate-hacking-case.

- Offenses: One count of conspiracy to commit computer fraud, two counts of computer fraud
- Guidelines Range: 63-78 months
- Sentence: 63 months

4. *United States v. Laoutaris*, 3:13-cr-00386-B-1 (N.D. Tx. Apr. 15, 2016)

Anastasio Laoutaris, who was an IT engineer for Locke Lord LLP from 2006 to August 2011, accessed the law firm's computer network without authorization on two occasions in December 2011. On both occasions, he issued instructions and commands that caused significant damage to the network, including deleting or disabling hundreds of user accounts, desktop and laptop accounts, and email accounts. Although there was no evidence that Laoutaris stole any data from the firm, his conduct seems likely to have prevented firm attorneys from accessing their network or email accounts, thereby prejudicing the firm's clients as well. Laoutaris also received an obstruction-of-justice enhancement based on his testimony at trial. *See* Judgment (Dkt. 103); Press release, https://www.justice.gov/usao-ndtx/pr/former-law-firm-it-engineer-convicted-computer-intrusion-case-sentenced-115-months.

- Offenses: Two counts of computer fraud
- Guidelines Range: 97-121 months
- Sentence: 115 months

5. *United States v. Correa*, 4:15-cr-00679 (S.D. Tx. July 18, 2016)

While working as Director of Baseball Development for the St. Louis Cardinals, Christopher Correa illicitly accessed the Houston Astros' private online database and email accounts to gain access to Astros proprietary information. During 2013, he was able to access Astros' scout rankings of every player eligible for the draft. He also viewed, among other things, an Astros weekly digest page, which described the performance and injuries of prospects the Astros were considering, as well as scouting

notes on those prospects. During the June 2013 amateur draft, Correa viewed information on players drafted by the Astros and other teams. Correa also leaked stolen data to Sports Illustrated and Deadspin to embarrass the Astros. *See* Plea Agreement (Dkt. 15); United States' Sentencing Memorandum (Dkt. 45-2); Judgment (Dkt. 48); Press release, https://www.justice.gov/opa/pr/former-cardinals-official-sentenced-prison-astros-computer-intrusions.

- Offenses: Five counts of computer fraud
- Guidelines Range: 46-57 months
- Sentence: 46 months

6. *United States v. Livingston*, 2:15-cr-00626-WJM (D.N.J. Feb. 14, 2017)

Timothy Livingston operated a business that specialized in sending spam emails on behalf of its clients. Beginning in January 2012, Livingston solicited an associate to write computer programs that would send spam in a manner that concealed the true origin of the email and bypassed filters. Livingston also used botnets, proxy servers, and corporate mail servers, and hacked into individual email accounts to further his spam campaigns, which enabled him to send out massive amounts of spam without identifying himself as the sender. *See* Judgment (Dkt. 76); Press release, https://www.justice.gov/usao-nj/pr/florida-man-sentenced-four-years-prison-hacking-spamming-scheme-used-stolen-email.

- Offenses: One count of conspiracy to commit computer fraud, one count of conspiracy to commit email fraud, one count of aggravated identity theft
- Guidelines Range: 57-71 months
- Sentence: 48 months

7. *United States v. Lostutter*, 5:16-cr-00062 (E.D. Ky. Mar. 8, 2017)

Deric Lostutter and a coconspirator hacked into a website, created by a fan of a Steubenville High School sports teams, to bring attention to a rape for which two Steubenville High School football players had been arrested in August 2012, and at the time were being held in custody. Lostutter wrote a manifesto and filmed a video threatening to reveal personal identifying information of Steubenville High School students and claiming falsely that the administrator of the fan website was involved in child pornography and directed a "rape crew." As part of the same hack, Lostutter and his coconspirator

accessed the administrator's private email account, and then publicly posted a link to download the administrator's emails on the fan website. Lostutter and his coconspirator changed the website so no one could access anything regarding athletics and could only view the video, the manifesto, and the link to the administrator's private emails. *See* United States' Sentencing Memorandum (Dkt. 101); Judgment (Dkt. 109); Press release, https://www.justice.gov/usao-edky/pr/winchester-man-sentenced-24-months-illegally-hacking-website-and-lying-federal-agents.

- Offenses: One count of conspiracy to commit computer fraud, one count of false statements
- Guidelines Range: 18-24 months
- Sentence: 24 months

8. *United States v. Fernandez*, 14-cr-0277-GPC (S.D. Cal. Jan. 19, 2018)

Between 2011 and 2014, Victor Fernandez and his coconspirators were part of a Tijuana-based conspiracy that hacked the computer servers of major U.S. mortgage brokers, stole over 4,200 customers' mortgage applications, and then used the victims' social security numbers, addresses, dates of birth, and personal information to open unauthorized lines of credit and take over and drain victims' retirement and brokerage accounts. The offenses victimized approximately 250 individuals, who suffered losses totaling between $400,000 and $1 million. *See* United States' Sentencing Memorandum, (Dkt. 254); Judgment (Dkt. 264); Press release, https://www.justice.gov/usao-sdca/pr/chula-vista-man-sentenced-computer-hacking-and-wire-fraud-scheme.

- Offenses: One count of conspiracy to commit bank fraud, one count of computer fraud, and one count of aggravated identity theft
- Guidelines Range: 130-162 months
- Sentence: 129 months

III. DISCUSSION

The United States recommends a sentence of 94 months imprisonment. That recommendation is based on the Sentencing Guidelines (low end, plus 2 years consecutive for the § 1028A counts), which incorporate the factors of 18 U.S.C. § 3553(a), including "the need to avoid unwarranted sentence disparities among defendants with similar records who have been found guilty of similar conduct." *Id.* § 3553(a)(6).

In developing the Sentencing Guidelines and in refining them through years of amendments, the Sentencing Reform Act requires the Sentencing Commission to consider a number of factors, including the same § 3553(a) factors and the need for "reducing unwarranted sentence disparities." 28 U.S.C. § 994(b)(1)(f); *see also United States v. Peach*, 356 F. Supp. 2d 1018, 1021 (D.N.D. 2005) (quoting 2005 testimony of Judge Ricardo H. Hinojosa, Chair of the United States Sentencing Commission, before Congress, as stating "the factors the Sentencing Commission has been required to consider in developing the Sentencing Guidelines are a virtual mirror image of the factors sentencing courts are required to consider pursuant to 18 U.S.C. § 3553(a) and the *Booker* decision"). The Supreme Court has thus stated, "avoidance of unwarranted disparities was clearly considered by the Sentencing Commission when setting the Guidelines ranges." *Gall v. United States*, 552 U.S. 38, 54 (2007); *see also United States v. Treadwell*, 593 F.3d 990, 1011 (9th Cir. 2010) (quoting *Gall* for same proposition).

Indeed, the Sentencing Guidelines provide information and guidance that are critical to avoiding unwarranted sentence disparities. The Sentencing Guidelines are the product of years of nationwide experience, sustained study, and fine-tuning. As stated by Justice Breyer, the "Sentencing Commission will continue to collect and study appellate court decisionmaking. It will continue to modify its Guidelines in light of what it learns, thereby encouraging what it finds to be better sentencing practices. It will thereby promote uniformity in the sentencing process." *United States v. Booker*, 543 U.S. 220, 263 (2005) (Breyer, J.). As such, "the post-*Booker* federal sentencing scheme aims to achieve uniformity by ensuring that sentencing decisions are anchored by the Guidelines and that they remain a meaningful benchmark through the process of appellate review." *Peugh v. United States*, 569 U.S. 530, 541 (2013); *see also Gall*, 552 U.S. at 50 (stating that "district courts must begin their analysis with the Guidelines and remain cognizant of them throughout the sentencing process").

In this case, an analysis of the data from the Sentencing Commission described in Section I above and the sentences described in Section II above confirms that the Guidelines range does what was

intended. The Guidelines range incorporates the § 3553(a) analysis with respect to the offense,[7] and there is no reason to depart from the Guidelines based on an unwarranted sentence disparity.

A. Sentencing Commission Data

In this case, the Sentencing Commission data described in Section I above shows that the significant sentence of imprisonment recommended by the United States for Defendant Baratov is in line with the sentences imposed on "defendants with similar records who have been found guilty of similar conduct." 18 U.S.C. § 3553(a)(6). First, of the 14 non-government-sponsored sentences, 11 of them were within or above the Guidelines (ranging from 18 months to 3708 months). In contrast, there were only three sentences that were below the Guidelines without being government-sponsored, and two of those sentences did not show substantial downward variances, *i.e.*, 51 months imposed from range of 63-78, and 72 months imposed from range of 92-115. The Sentencing Commission data thus shows that absent a government-sponsored justification, courts have generally sentenced defendants, whose § 2B1.1 offense conduct involves sophisticated means and committing an offense under 18 U.S.C. § 1030 to obtain personal information, to imprisonment terms within or near the Sentencing Guidelines range.

Second, based strictly on the numbers, the 94-month imprisonment recommendation of the United States for Defendant Baratov (who, as set forth in his guilty plea, took orders from paying customers to hack into accounts of 11,000 specifically-targeted victims) does not result in an unwarranted sentence disparity. The table below shows the non-government-sponsored sentences from the data described in Section I above and ranks them from longest to shortest prison sentence (with alternative incarceration less than imprisonment).

Loss Increase, 2B1.1(b)(2)	Final Offense Level	Final Criminal History Category	Prison Sentence	*Longest (1) to Shortest (14) Prison Sentence*
+8	23	1	72	*4*
+4	19	4	48	*9*
+6	15	1	42	*11*
+22	43	6	3708	*1*
+18	26	1	51	*8*

[7] Of course, the § 3553(a) factors also require that the Court consider offender characteristics. As described in the previously-filed government memoranda, Defendant Baratov's characteristics—including, among others, enjoying a loving, stable, and supportive upbringing and demonstrating a long-running and repetitive lack of concern with the personal harm he caused his victims—do not argue for leniency or create any disparity.

Loss Increase, 2B1.1(b)(2)	Final Offense Level	Final Criminal History Category	Prison Sentence	*Longest (1) to Shortest (14) Prison Sentence*
0	22	1	132	*2*
+6	14	3	45	*10*
0	12	1	Alt. 18	*13*
+8	21	1	72	*4*
+16	31	4	120	*3*
0	13	1	60	*7*
+12	19	1	Alt. 6	*14*
+4	13	1	18	*12*
+16	26	4	72	*4*

While the number of data points is modest, the 94-month sentence recommended in this case is in line with these sentences. For example, the rows highlighted in green show the spectrum between the longest (309 years of imprisonment) and shortest (6 months of alternative incarceration). The rows highlighted in blue show the spectrum between the second longest (132 months of imprisonment) and second shortest (18 months of alternative incarceration). The average of all 14 sentences is 318 months of imprisonment.[8] The average without the two endpoints (*i.e.*, 12 sentences between blue rows) is 62.5 months of imprisonment.[9] As detailed previously in the United States Sentencing Memorandum, Docket No. 36, at 10-14, Defendant Baratov's egregious, extensive, and reprehensible conduct makes it necessary that his sentence fall on the serious side of the spectrum.

Third, filtering the data further to match Defendant Baratov shows that the 94-month recommended range is sufficient, but not greater than necessary, and results in no unwarranted sentence disparity. As the parties and Probation agree, Defendant Baratov has a final offense level of 27 and a final Criminal History Category of I. There are four non-government-sponsored sentences from the Sentencing Commission data described in Section I above that have a final offense level of 20 or more and a final Criminal History Category of I. Those sentences follow below, and average 81.75 months.[10]

Loss Increase, 2B1.1(b)(2)	Final Offense Level	Final Criminal History Category	Prison Sentence
+8	23	1	72
+18	26	1	51
0	22	1	132

[8] 4452/14 = 318.
[9] 750/12 = 62.5.
[10] 327/4 = 81.75.

Loss Increase, 2B1.1(b)(2)	Final Offense Level	Final Criminal History Category	Prison Sentence
+8	21	1	72

Based on Defendant Baratov's agreed-upon final offense level (*i.e.*, 27), which is higher than that in any of these examples, his conduct justifies the moderately more-severe sentence than the average of these four that the government seeks.

To the extent that the defense argues about the government-sponsored below-Guideline sentences described in Section I above (rows in light grey), those sentences do not suggest unwarranted disparities. There are a variety of different reasons that could justify a government-sponsored below-Guidelines sentence, such as substantial assistance, and as discussed in the previously filed sentencing memoranda of the United States, there are no such reasons here. The difficulty of discerning the reasons and the extent of the downward variances based on those reasons magnifies the issue even further. Moreover, even with the government-sponsored below-Guidelines sentences, the 94-month recommendation in this case results in no unwarranted sentence disparity. For example, the average sentence of all 19 sentences described in Section I above is 255.1 months of imprisonment.[11] Excluding longest and shortest sentence, the average sentence is 66.7 months of imprisonment.[12] Filtering the data further to match Defendant Baratov in the table below (*i.e.*, sentences with a final offense level of 20 or more and a final Criminal History Category of I) shows that the 94-month recommended sentence falls reasonably on the serious side of the spectrum of the sentences imposed on similarly situated defendants.

Loss Increase, 2B1.1(b)(2)	Final Offense Level	Final Criminal History Category	Prison Sentence
+8	23	1	72
+18	26	1	51
0	22	1	132
+8	21	1	72
+22	43	1	72
+22	43	1	12.03[13]
+24	40	1	156
+12	31	1	54

[11] 4848/19 = 255.1
[12] 1134/17 = 66.7.
[13] The sentence in this case included 6 months of alternative incarceration.

B. Sentences from Other Sources

The sentences identified in hacking cases and described in Section II above also show that the 94-month recommendation of the United States presents no unwarranted disparity with the sentences imposed on "defendants with similar records who have been found guilty of similar conduct." 18 U.S.C. § 3553(a)(6). There is no precedent that is really parallel with this case—Defendant Baratov victimized people in quantities typical of a carder, but as described below caused personal and intimate harm not before seen in such scope. In aggregate, though, the sentences described show that the imposition of a Guidelines sentence in this case does not result in an unwarranted disparity for several reasons:

First, Defendant Baratov's case is not a carding case. The defendant did not hack into a network or a handful of networks to steal *en masse* and misuse credit card numbers. Rather, the defendant specifically marketed to, took orders from, customers whose interest in the victims' email account contents was sufficiently focused and specific that it would lead them to enter into a criminal conspiracy with Defendant Baratov in order to gain such access (*i.e.*, the crimes were premeditated and not of opportunity). Once Defendant Baratov's open desire for money was matched up with a customer's desire to intrude into a specific victim's personal lives, the defendant specifically targeted identified victims, deceived those victims to hand over the passwords to the private digital records in their webmail accounts, and sold that stolen access to those customers. His customers could then exploit those victims for any number of purposes beyond mere credit card misuse (including theft of personal images, savings, contacts, and access to business associates and family). As a result, Defendant Baratov's 11,000 victims reflect 11,000 separate decisions to expose an individual's most personal, intimate, and valuable information in exchange for cash. Whether or not Defendant Baratov knew the identities or desires of particular customers, it was foreseeable to him that the nature of his crime involved the exposure of personal information to those with a motive to hurt the victims in some way.

In contrast to defendants charged in carding cases, Defendant Baratov enabled his customers to exploit personal data and to exact greater financial harms and more significant and lasting personal harms, such as in the examples discussed in the non-carding cases described in Section II.B above. For example, as previously described in the United States' Sentencing Memorandum, Victim 1 stated that he lost business correspondence and copyrighted items, Victim 2 stated that the potential for damage

constantly disturbs him, and Victim 3 reported losing a client when Victim 3's account was used to distribute private information and photographs of Victim 3's client. US Sent. Mem. (Docket No. 36), at 7-8. If anything, the Guidelines' loss amount calculation of $500 per hacked email account understates the lasting harm that each of Baratov's victims has suffered and continues to suffer.

Second, for the non-carding cases described in Section II.B above, the sentences imposed show that courts generally sentence within or near the Sentencing Guidelines range. Among the eight examples described in Section II.B above, five were within (*Makawana*, *Musacchio*, *Laoutaris*, *Correa*, *Lostutter*) and one was above (*Chaney*, with particularly invasive conduct) the Guidelines range. The two sentences that were below the Guidelines range did not show substantial downward variances (48 months imposed from 57-71 in *Livingston*; and 129 months imposed from 130-162 in *Fernandez*). This observation (*i.e.*, sentencing at or near the Guidelines range) tracks that identified by the Sentencing Commission data analysis in Section III.A above.

Third, this general following of the Guidelines range is an implicit recognition that the Sentencing Guidelines appropriately reflect the § 3553 factors and result in *warranted* disparities. The *Makwana* and *Laoutaris* defendants, for example, both attempted to cause damage to their respective former employers. The *Makwana* defendant attempted, but failed to do so, and was sentenced to 41 months (low end of the Guidelines). The *Laoutaris* defendant succeeded in damaging his former employer and obstructed justice, and a higher 115-month sentence (higher-end of the Guidelines) was imposed. Similarly, the *Musacchio* and *Correa* defendants both attempted to exploit information from their respective competitors. The *Correa* defendant viewed Astros baseball scouting rankings to benefit his work for the Cardinals, leaked that information to embarrass the Astros, and was sentenced to 46 months (low end of the Guidelines). The *Musacchio* defendant went further (by abusing his former position of leadership in his competitor, enlisted the help of two others, and used the stolen information for corporate economic espionage and self-enrichment) and was sentenced to a higher 63-month sentence (low end of his Guidelines range).

Fourth, downward departures appear to coincide with cases in which specific victims are *not* targeted. In the non-carding cases described in Section II.B above, for example, the two below Guidelines sentences were in *Livingston* (where the defendant appropriated email accounts to send more

spam emails on behalf of his business) and in *Fernandez* (where the defendant saw targets of opportunity and used *en masse* stolen mortgage applications to pen unauthorized lines of credit and drain victim accounts). Similarly, in carding cases described in Section II.A above, the sentences imposed show that courts may often sentence below the Guidelines range where defendants steal and misuse credit card numbers *en masse* – not to target a specifically identified victim.[14]

By the same token, the sentences within or above the Guidelines in the non-carding cases described in Section II.B above are all cases in which the defendants targeted specific victims. The *Makwana* and *Laoutaris* defendants targeted the networks of their former employers, the *Musacchio* and *Correa* defendants targeted information from their competitors, the *Chaney* defendant targeted the personal email accounts of mostly celebrities, and the *Lostutter* defendant targeted a particular website and its administrator. This is the spectrum of targeting that Defendant Baratov facilitated with his customers, and the reason why a sentence within the Guidelines range is appropriate in this case.

In this context, the defendant's citations to *Hatala*, *Collins*, and *Majerczyk* do not justify a downward variance from the Guidelines range in this case.[15] *United States v. Hatala*, 1:12-CR-912-KBF (SDNY February 13, 2013) was a carding case in which the defendant hacked into customer databases in an attempt to steal username and passwords that could be used to access PayPal accounts. The *Hatala* defendant did not target particular victims, and while the defendant had bulk lists of stolen credentials, the United States had evidence to verify only 300 credentials as actually working on PayPal. Pursuant to the *Hatala* plea agreement—with the loss based on those 300 credentials—the Guideline range was 18-24 months. Exhibit F to Def. Sent. Memo. (Docket No. 37-6). In advance of the sentencing, the Court notified the parties that it was considering an upward departure based on "the scope and scale, invasive nature, level of planning and intentional conduct, and duration of the offense."

---

[14] By analogy to credit card offenses, the Sentencing Commission's Quick Facts publication for fiscal year 2016 states that the average sentence for credit card offenses was 28 months. Approximately 51.6% of the sentences were within the Guidelines range, and 26.2% were non-government-sponsored below Guidelines sentences. Quick Facts on Federal Credit Card Offenses, *available at* https://www.ussc.gov/sites/default/files/pdf/research-and-publications/quick-facts/Credit_Card_Fraud_FY16.pdf. The Sentencing Commission does not appear to have any Quick Facts publications for computer fraud and abuse cases.

[15] As previously noted in the United States Response Memorandum, the *Hatala*, *Collins*, and *Majerczyk* defendants were each sentenced to within or above their respective Guidelines ranges. US Resp. Mem. (Docket No. 39), at 8.

Exhibit G to Def. Sent. Memo. (Docket No. 37-7), at Entry #17. The Court sentenced Hatala to 30 months, above the Guideline range. *Id.*, at Entry #22.

Defendant Baratov's conduct is much more egregious than Hatala's. Defendant Baratov hacked into more than 11,000 accounts (*i.e.*, over 35 times what Hatala was sentenced for). As further agreed in his Plea Agreement, Defendant Baratov employed sophisticated means and engaged in hacking to obtain personal information, both of which support a higher Guidelines range and sentence. Unlike Hatala, Defendant Baratov engaged in the repeated and targeted hacking of personal information—at least 11,000 times—for his own self-enrichment. The only apt comparison to *Hatala* is that Defendant Baratov's offense conduct exhibited the attributes that justified the upward departure in that case.

Notably, the policy of sentencing those who steal personal information more severely is incorporated into the Guidelines. In 1997, for example, the Sentencing Commission amended § 2B1.1 to state explicitly that upward departures may be appropriate for "a substantial invasion of a privacy interest." Amendment 551 to USSG (adding language now contained in Application Note 20(A)(ii) of § 2B1.1). In 2003, the Sentencing Commission added the 2-level enhancement for computer fraud and abuse offenses involving an intent to obtain personal information pursuant to the Cyber Security Enhancement Act of 2002, 6 U.S.C. § 145 (directing Guidelines to reflect, in part, the "growing incidence of such [18 U.S.C. § 1030] offenses"). Amendment 654 to USSG (stating that reason for amendment was to address "the serious harm and invasion of privacy that can result from offenses involving the misuse of, or damage to, computers"). In 2011, the Sentencing Commission amended that 2-level enhancement to ensure that computer fraud and abuse offenses involving personal information would result in its own additional incremental increase over any others harms pursuant to the Identity Theft Enforcement and Restitution Act of 2008. Amendment 726 to USSG. It is proper, then, for this and the other reasons described that Hatala received a lower sentence than that the government recommends for Defendant Baratov.

Similarly, the defendant's citations to *United States v. Ryan Collins*, 16-CR-121 (M.D.Pa. Oct. 26, 2016), and *United States v. Majerczyk*, 16-CR-550 (N.D.Ill. Feb. 6, 2017) are unavailing. As with Defendant Baratov, the *Collins* and *Majerczyk* defendants each engaged in phishing schemes that allowed them to deceive their victims into handing over their passwords. In that sense, they are all non-

carding cases. Defendant Baratov's conduct, however, was more egregious. He hacked more victim accounts, sold his stolen access to the customers who targeted those victims for untold nefarious purposes, and did not limit himself or his customers to voyeurism (as exhibited, for example, by his interactions with a self-described hit man).

The *Majerczyk* defendant accessed 30 accounts, through which he was able to access personal data including nude photographs and videos of 300 victims to "see things through other people's eyes" and "for kicks." Exhibit D to Def. Sent. Mem. (Docket No. 37-4). The *Collins* defendant accessed personal data including nude photographs of 600 victims "for sexual gratification." Exhibit B to Def. Sent. Mem. (Docket No. 37-2). Neither defendant distributed any of the personal data that they hacked. *Id.* (stating that Collins "did not share or exchange the private materials that he obtained"); Sentencing Transcript of *United States v. Majerczyk*, 16-CR-550 (N.D.Ill.), Docket No. 28, at 8 (stating that an unusual factor "about this particular case and this particular defendant [Majerczyk] is that it does not appear that he disseminated this information further"). Additionally, while Probation in *Collins* and *Majerczyk* found the agreed-upon Guidelines ranges had errors and were too low, the United States requested that the Court "give the defendant the benefit of the bargain" in each case.[16] Exhibits B and D to Def. Sent. Mem. (Docket Nos. 37-2 and 37-4). The *Majerczyk* defendant was sentenced to 9 months imprisonment as recommended; the *Collins* defendant was sentenced to 18 months imprisonment as recommended. Exhibits B, C, D, E to Def. Sent. Mem. (Docket Nos. 37-2 to 37-5).

By contrast, Defendant Baratov hacked into more than 11,000 victim accounts. Defendant Baratov's criminal conduct thus violated approximately 10,000 more victims than the *Collins* and *Majerczyk* defendants did combined. That fact alone (and it is not alone) warrants a far more serious sentence. For example, the *Majerczyk* defendant received a 9-month sentence for hacking into 300 victims; the *Collins* defendant received double that sentence (*i.e.*, 18 months) for hacking into twice as

[16] Note that the Ninth Circuit held in *United States v. Banuelos-Rodriguez*, 215 F.3d 969 (9th Cir. 2000) (en banc) that disparities between the charging and plea-bargaining decisions of United States Attorneys in different federal districts was not a proper ground for departing from an otherwise applicable Guideline range. *Id.* (affirming district court denial of downward departure based on different "fast track" programs for illegal reentry defendants in C.D. Cal. and S.D. Cal.); *see also United States v. Hernandez-Franco*, 455 F. App'x 790, 791 (9th Cir. 2011) (unpublished) (affirming sentence, rejecting argument that intra-district disparity warranted lower sentence, and citing Banuelos-Rodriguez).

many victims (*i.e.*, 600). By this metric, Defendant Baratov would receive a sentence of 330 months imprisonment.[17] However, the United States is recommending less than a third of that: 94 months of imprisonment (*i.e.*, approximately 10 times the *Majerczyk* sentence) for Defendant Baratov hacking more than 11,000 victims (*i.e.*, approximately 36 times the number of *Majerczyk* victims).

Unlike the defendants in *Collins* and *Majerczyk*, Defendant Baratov solicited orders from his customers to hack specific victims and disseminated the hacked passwords to those customers to exploit consistent with their own plans. *See, e.g.*, Sentencing Transcript of *United States v. Majerczyk*, 16-CR-550 (N.D.Ill.), Docket No. 28, at 23 (Court stating to defendant that "[t]he fact that there was no, at least, evidence of dissemination works in your favor"). In the *Chaney* sentencing described in Section II.B above, for example, the defendant was sentenced to 120 months (above the Guidelines range of 57-71) months for hacking into the personal email accounts of approximately 60 people and disseminating intimate photographs to third-party websites, which caused one of those victims to attempt suicide.

In short, none of these cases cited by the defendant supports the proposition that the Sentencing Guidelines that he agreed to in this case overstate the appropriate sentence under 18 U.S.C. § 3553(a). The Sentencing Commission data described in Section I above and the cases described in Section II above show that the sentence of imprisonment recommended by the United States (and Probation) for Defendant Baratov is consistent with the sentences imposed on "defendants with similar records who have been found guilty of similar conduct." 18 U.S.C. § 3553(a)(6).

* * *

[17] 11,000 accounts / 300 accounts * 9 months = 330 months.

Accordingly, in full consideration of the Sentencing Guidelines and the factors enumerated in 18 U.S.C. § 3553(a), the United States respectfully recommends that the Court impose a sentence of 70 months imprisonment for Count One, 24 months consecutive imprisonment for Counts Forty through Forty-Seven, 3 years supervised release, and restitution and fine amounts that encompass any and all of his assets.

Respectfully submitted,

ALEX G. TSE
Acting United States Attorney

DATED: May 8, 2018

/s/ Jeffrey Shih
JEFFREY SHIH
Assistant United States Attorney

SCOTT K. MCCULLOCH
EVAN TURGEON
Trial Attorneys, National Security Division